Average Multiplicative Order of Finitely Generated Subgroup of Rational Numbers Over Primes

Cihan Pehlivan*

Dipartimento di Matematica, Università Roma Tre,
Largo S. L. Murialdo, 1, I–00146 Roma Italia

May 5, 2015

arXiv:1504.01550v2 [math.NT] 2 May 2015

Abstract

Given a finitely generated multiplicative subgroup $\Gamma \subseteq \mathbb{Q}^*$, assuming the Generalized Riemann Hypothesis, we determine an asymptotic formula for average over prime numbers, powers of the order of the reduction group modulo p. The problem was considered in the case of rank 1 by Pomerance and Kurlberg. In the case when Γ contains only positive numbers, we give an explicit expression for the involved density in terms of an Euler product. We conclude with some numerical computations.

1 Introduction

Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup. The *support* of Γ is the (finite) set of primes p for which the p–adic valuation $v_p(g) \neq 0$ for some $g \in \Gamma$. We denote this set by $\operatorname{Supp}\Gamma$ and define $\sigma_\Gamma = \prod_{p\in \operatorname{Supp}\Gamma} p$. For each prime $p \nmid \sigma_\Gamma$, it is well defined the reduction of Γ modulo p. That is

$$\Gamma_p = \{g \pmod p : g \in \Gamma\}. \tag{1}$$

For simplicity, when p does divide the support of Γ , we let $\Gamma_p = \{1\}$. We also denote by $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ the extension of the cyclotomic field $\mathbb{Q}(\zeta_k)$ obtained by adding the k–th roots of all the elements in Γ. We denote Jordan's totient function by

$$J_r(m) := m^r \prod_{\ell \mid m} \left(1 - \frac{1}{\ell^r}\right) \tag{2}$$

and sum of t–th power of positive divisors of n by

$$\sigma_t(n) := \sum_{d\mid n} d^t. \tag{3}$$

Theorem 1. *Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup with rank $r \geq 2$ and assume that the Generalized Riemann Hypothesis holds for $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ $(k \in \mathbb{N})$. Let*

$$C_{\Gamma,t} := \sum_{k\geq 1} \frac{J_t(k)(\operatorname{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]} \tag{4}$$

*pehlivan@mat.uniroma3.it

where $\mathrm{rad}(k)$ *denotes the product of distinct prime numbers dividing* k*. Then the series* $C_{\Gamma,t}$ *converges absolutely and as* $x \to \infty$*,*

$$\sum_{p \le x} |\Gamma_p|^t = \mathrm{li}(x^{t+1}) \left(C_{\Gamma,t} + O_\Gamma\left(\frac{\log\log x}{(\log x)^r} \right) \right) \tag{5}$$

and the constant implied by the O_Γ*–symbol may depend on* Γ*.*

Further on, for the case $t = 1$ we use C_Γ instead of $C_{\Gamma,1}$. Kurlberg and Pomerance in [3] consider the case when $\Gamma = \langle g \rangle$ has rank 1. In the special case when $\Gamma \subset \mathbb{Q}^+$, we express the value of C_Γ as an Euler product. To this purpose, we introduce some notations:

- If $\eta \in \mathbb{Q}^*$, by $\delta(\eta)$ we denote the *field discriminant* of $\mathbb{Q}(\sqrt{\eta})$.
- For any $k \in \mathbb{N}^+$, $\Gamma(k) = \Gamma \cdot \mathbb{Q}^{*k}/\mathbb{Q}^{*k}$.

For any square-free integer η, let

$$t_\eta = \begin{cases} \infty & \text{if for all } t \ge 0,\ \eta^{2^t}\mathbb{Q}^{*2^{t+1}} \notin \Gamma(2^{t+1}) \\ \min\{t \in \mathbb{N} : \eta^{2^t}\mathbb{Q}^{*2^{t+1}} \in \Gamma(2^{t+1})\} & \text{otherwise.} \end{cases}$$

We will show the following:

Theorem 2. *Assume that* Γ *is a finitely generated subgroup of* $\mathbb{Q}^+$*. Then*

$$\begin{aligned} C_{\Gamma,t} &= \prod_p \left(1 - \sum_{\alpha \ge 1} \frac{p^t - 1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)} \right) \\ &\times \left(1 + \sum_{\substack{\eta \mid \sigma_\Gamma \\ \eta \ne 1}} S_\eta \prod_{p \mid 2\eta} \left(1 - \left(\sum_{\alpha \ge 1} \frac{p^t - 1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)} \right)^{-1} \right)^{-1} \right) \end{aligned} \tag{6}$$

where

$$S_\eta = \frac{\displaystyle\sum_{\alpha \ge \gamma_\eta} \frac{2^t - 1}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|}}{\displaystyle\sum_{\alpha \ge 1} \frac{2^t - 1}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|}} \tag{7}$$

and $\gamma_\eta = \max\{1 + t_\eta, v_2(\delta(\eta))\}$*.*

A calculation shows that, in the case when $\Gamma = \langle g \rangle$, the above expression for $C_{\langle g \rangle}$ coincides with that of Kurlberg and Pomerance. In the special case when Γ consists of prime numbers and $t = 1$, the above formula can be considerably simplified:

Corollary 3. *Let* $\Gamma = \langle p_1, \ldots, p_r \rangle$ *where all the* p_i*'s are prime numbers and* $r \ge 1$*, with the notation above, we have*

$$\begin{aligned} C_{\langle p_1,\ldots,p_r \rangle} &= \prod_p \left(1 - \frac{p}{p^{r+2} - 1} \right) \\ &\times \left(1 + \sum_{\substack{\eta \mid p_1 \cdots p_r \\ \eta \ne 1}} \frac{1}{2^{\max\{0, v_2(\delta(\eta)/2)\}(r+2)}} \prod_{\ell \mid 2\eta} \frac{\ell}{\ell + 1 - \ell^{r+2}} \right). \end{aligned} \tag{8}$$

The quantity

$$C_r = \prod_p \left(1 - \frac{p}{p^{r+2} - 1}\right) \tag{9}$$

can be computed with arbitrary precision:

r	C_r
1	$0.57595996889294543964316337549249669251 \cdots$
2	$0.82357659279814332395380438513901050177 \cdots$
3	$0.92190332088740008067545348360869076931 \cdots$
4	$0.96388805107176946676374437726734997946 \cdots$
5	$0.98282912014687261524345691713313004185 \cdots$
6	$0.99168916383630008819101294319807859837 \cdots$
7	$0.99593155027181927318700546733612700362 \cdots$
8	$0.99799372275691129752727433560285572887 \cdots$
9	$0.99900593591154969071253065973483263501 \cdots$
10	$0.99950593624928276115384423618416539651 \cdots$

Furthermore, we have the following corollary.

Corollary 4. *Let Γ be a finitely generated subgroup of $\mathbb{Q}^+$ with rank r. Then C_Γ is a non zero rational multiple of C_r.*

We conclude the paper with some numerical evidence. Complete account of the results in this stream we reefer the survey of P. Moree [5].

2 Notational conventions

Throughout the paper, the letter p always denote *prime numbers.* As usual, we use $\pi(x)$ to denote the *number of* $p \leq x$ and

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} \tag{10}$$

denotes the *logarithmic integral* function. The invariant $\Delta_r(\Gamma)$ of a multiplicative subgroup $\Gamma \subseteq \mathbb{Q}^*$ with $\mathrm{rank}_{\mathbb{Z}}(\Gamma) = r$ is defined as the greatest common divisor of all the minors of size r of the relation matrix of the group of Γ (see [1, Section 3.1] for some details).

φ and μ are respectively the *Euler* and the *Möbius* functions. An integer is said *squarefree* if it is not divisible for the square of any prime number. If $\eta \in \mathbb{Q}^*$, by $\delta(\eta)$ we denote the *field discriminant* of $\mathbb{Q}(\sqrt{\eta})$. So, if $\eta \in \mathbb{Z}$ is square-free, $\delta(\eta) = \eta$ if $\eta \equiv 1 \pmod 4$, and $\delta(\eta) = 4\eta$ otherwise. For $\alpha \in \mathbb{Q}^*$ we denote by $v_\ell(\alpha)$ the *ℓ–adic valuation* of α.

For functions F and $G > 0$ the notations $F = O(G)$ and $F \ll G$ are equivalent to the assertion that the inequality $|F| \leq c\,G$ holds with some constant $c > 0$. We write $F \sim G$ if $\lim_{x\to\infty} \frac{F(x)}{G(x)} = 1$. In what follows, all constants implied by the symbols O and $\ll$ may depend (when obvious) on the small real parameter ϵ but are absolute otherwise; we write O_λ and $\ll_\lambda$ to indicate that the implied constant depends on a given parameter λ. We also define the index of subgroup $\mathrm{ind}(\Gamma_p) = \frac{p-1}{|\Gamma_p|}$.

3 Lemmata

In this section we present some results which we need for proof of the main theorem. The following Lemma describes explicitly the degree of $[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]$ (see [6, Lemma 1 and Corollary 1]).

Lemma 5. *Let $k \geq 1$ be an integer. With the notation above, we have*

$$\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)\right] = |\Gamma(k)|/|\widetilde{\Gamma}(k)|$$

where

$$\widetilde{\Gamma}(k) = (\Gamma \cap \mathbb{Q}(\zeta_k)^{2^{v_2(k)}}) \cdot \mathbb{Q}^{*2^{v_2(k)}}/\mathbb{Q}^{*2^{v_2(k)}}. \tag{11}$$

Furthermore, in the special case when $\Gamma \subset \mathbb{Q}^+$,

$$\widetilde{\Gamma}(k) = \{\eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}}\mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta) \mid k\}. \tag{12}$$

The following statement is obtained using the effective version of the Chebotarev Density Theorem due to Serre (see [7, Theorem 4]).

Lemma 6 (Chebotarev Density Theorem)**.** *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r and $k \in \mathbb{N}^+$. The GRH for the Dedekind zeta function of $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ implies that*

$$\#\{p \leq x : p \notin \operatorname{Supp}\Gamma,\ k \mid \operatorname{ind}(\Gamma_p)\} = \frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]} + O\big(\sqrt{x}\log(xk^{r+1}\sigma_\Gamma)\big). \tag{13}$$

The explicit formula for the degree $\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}\right]$ can be found in [6, Lemma 1]. The next results follows from Lemma 5 (see [6, Equation 7]).

Corollary 7. *Let $\Gamma \subset \mathbb{Q}^*$ be a subgroup of $r = \operatorname{rank}_{\mathbb{Z}}(\Gamma)$ and $k \in \mathbb{N}$. Then*

$$2k^r \geq [\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)] \geq \frac{(k/2)^r}{\Delta_r(\Gamma)}. \tag{14}$$

Next Lemma is implicit in the work of C. R. Matthews (see [4]).

Lemma 8. *Assume that $\Gamma \subseteq \mathbb{Q}^*$ is a multiplicative subgroup of rank $r \geq 2$ and assume that $(a_1, \ldots, a_r)$ is a $\mathbb{Z}$–basis of Γ. Let $t \in \mathbb{R}$, $t > 1$. We have the following estimate*

$$\#\{p \notin \operatorname{Supp}\Gamma : |\Gamma_p| \leq t\} \ll_\Gamma \frac{t^{1+1/r}}{\log t}. \tag{15}$$

Theorem 9. *Assume the GRH. Let Γ be a multiplicative subgroup of $\mathbb{Q}^*$ of rank $r \geq 2$. Then, for $1 \leq L \leq \log x$, we have*

$$\#\left\{p \leq x : p \notin \operatorname{Supp}\Gamma, |\Gamma_p| \leq \frac{p-1}{L}\right\} \ll_\Gamma \frac{\pi(x)}{L^r}. \tag{16}$$

The proof of the above is routine and easier than the main theorem in [2] and to [3, Theorem 6]. Hence we will skip some of the details.

Proof. Let t, $L \leq t \leq x$ be a parameter that will be chosen later.

- *first step*: First consider primes $p \notin \operatorname{Supp}\Gamma$ such that $|\Gamma_p| \leq \frac{p-1}{t}$. By Lemma 8, we have

$$\#\left\{p \notin \operatorname{Supp}\Gamma : |\Gamma_p| \leq \frac{x}{t}\right\} \ll_\Gamma \frac{(x/t)^{1+1/r}}{\log(x/t)}. \tag{17}$$

- *second step*: Next consider the primes $p \notin \operatorname{Supp}\Gamma$ such that there exists a prime q, $L \leq q \leq t$ such that $q \mid \operatorname{ind}(\Gamma_p) = \frac{p-1}{|\Gamma_p|}$. If we apply Lemma 6, we obtain

$$\begin{aligned} \#\{p \leq x : p \notin \operatorname{Supp}\Gamma, q \mid \operatorname{ind}(\Gamma_p)\} &= \frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_q, \Gamma^{1/q}) : \mathbb{Q}]} + O_\Gamma\left(\sqrt{x}\log(xq)\right) \\ &\ll_\Gamma \frac{\pi(x)}{q^r \varphi(q)} + \sqrt{x}\log(xq) \end{aligned} \tag{18}$$

where in the latter estimate we have applied Corollary 7. If we sum the above over primes q: $L \leq q \leq t$, we obtain

$$\begin{aligned} &\#\{p \leq x : p \notin \operatorname{Supp}\Gamma, \exists q \mid \operatorname{ind}(\Gamma_p), L \leq q \leq t\} \\ &\ll_\Gamma \sum_{\substack{q \text{ prime} \\ L \leq q \leq t}} \left(\frac{\pi(x)}{q^r \varphi(q)} + \sqrt{x}\log(xq)\right) \ll_\Gamma \frac{\pi(x)}{L^r} + x^{1/2} t \log x. \end{aligned}$$

- *third step*: The primes p that were not counted in previous steps, have the property that all the prime divisors of $\operatorname{ind}(\Gamma_p)$ belong to the interval $[1, L]$. Hence, for such primes p, $\operatorname{ind}(\Gamma_p)$ is divisible for some integer d in $[L, L^2]$.

  Applying again Lemma 6 and Corollary 7, and taking the sum over d we deduce that the total number of such primes is

$$\ll_\Gamma \sum_{\substack{d \in \mathbb{N} \\ L < d \leq L^2}} \left(\frac{\pi(x)}{d^r \varphi(d)} + x^{\frac{1}{2}}\log(xd)\right) \ll_\Gamma \frac{\pi(x)}{L^r} + x^{1/2} L^2 \log x. \tag{19}$$

A choice of $t = \frac{x^{1/2}}{L^r \log^2 x}$ allows us to conclude the proof. $\square$

The Theorem of Wirsing [8] is formulated as follows.

Lemma 10. *Assume that a real valued multiplicative function $h(n)$ satisfies the following conditions.*

- $h(n) \geq 0, n = 1, 2, ..;$
- $h(p^n) \leq c_1 {c_2}^v, v = 2, 3...$, *for some constants c_1, c_2 with $c_2 < 2$;*
- *there exists a constant $\tau > 0$ such that*

$$\sum_{p \leq x} h(p) = (\tau + o(1))\frac{x}{\log x}. \tag{20}$$

Then for any $x \geq 0$,

$$\sum_{n \leq x} h(n) = \left(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1)\right)\frac{x}{\log x}\prod_{p \leq x}\sum_{\nu \geq 0}\frac{h(p^\nu)}{p^\nu} \tag{21}$$

where γ is the Euler constant, and

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt \tag{22}$$

is the gamma function.

4 Proof of the Theorem 2

Proof of Theorem 2. We start by splitting the sum $C_{\Gamma,t}$ as

$$C_{\Gamma,t} := \sum_{k\geq 1} \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]} = A_1 + A_2 \tag{23}$$

where A_1 is the sum of the terms corresponding to odd values of k and A_2 is the sum of the terms corresponding to even values of k. Note that if $\Gamma \subseteq \mathbb{Q}^+$ by Lemma 5 we have

$$[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}] = \frac{\varphi(k)|\Gamma(k)|}{|\widetilde{\Gamma}(k)|} \tag{24}$$

where, if k is even,

$$\widetilde{\Gamma}(k) = \{\eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}}\mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta)\mid k\} \tag{25}$$

while if k is odd $\widetilde{\Gamma}(k) = \{1\}$. We define

$$f_t(k) = \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}\varphi(k)|\Gamma(k)|}.$$

Note that if $D \in \mathbb{N}^+$ is even, since $f_t(k)$ is multiplicative in k, then

$$\sum_{\substack{k\geq 1\\ \gcd(k,D)=1}} f_t(k) = \prod_{p\nmid D}\left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p\nmid D}\left(1-\sum_{\alpha\geq 1}\frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right). \tag{26}$$

Therefore, we have the identity

$$A_1 = \prod_{p>2}\left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p>2}\left(1-\sum_{\alpha\geq 1}\frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right). \tag{27}$$

We can write A_2 as,

$$\begin{aligned}
A_2 &= \sum_{\eta\mid\sigma_\Gamma}\sum_{\substack{k\geq 1, 2\mid k\\ \widetilde{\Gamma}(k)\ni\eta}} \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}\varphi(k)|\Gamma(k)|}\\
&= \sum_{\eta\mid\sigma_\Gamma}\ \sum_{\substack{\alpha\geq 1\\ \eta^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)}}\ \sum_{\substack{k\geq 1\\ v_2(k)=\alpha\\ \delta(\eta)\mid k}} f_t(k)\\
&= \sum_{\eta\mid\sigma_\Gamma}\ \sum_{\substack{\alpha\geq 1\\ \eta^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)\\ \alpha\geq v_2(\delta(\eta))}} \frac{-(2^t-1))}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|}\sum_{\substack{k\geq 1\\ 2\nmid k\\ \delta(\eta)\mid 8k}} f_t(k).
\end{aligned} \tag{28}$$

Now write $\delta(\eta) = 2^{v_2(\delta(\eta))}M$. Then

$$\begin{aligned}
\sum_{\substack{k\geq 1\\ 2\nmid k\\ \delta(\eta)\mid 8k}} f_t(k) &= \prod_{\substack{p>2\\ p\nmid M}}\left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right)\prod_{\substack{p>2\\ p\mid M}}\left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)\\
&= A_1\prod_{\substack{p>2\\ p\mid M}}\left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right)^{-1}\left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)
\end{aligned} \tag{29}$$

Hence, if t_η is the quantity defined in (1), then

$$C_{\Gamma,t} := A_1 \times \left(1 + \sum_{\eta|\sigma_\Gamma} \sum_{\substack{\alpha\geq 1\\ \alpha\geq t_\eta+1\\ \alpha\geq v_2(\delta(\eta))}} \frac{-(2^t-1)}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|} \prod_{\substack{p>2\\ p|M}} \left(1 + \left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)^{-1}\right)^{-1}\right).$$

Now let

$$\delta_\Gamma := \prod_{p \text{ prime}} \left(1 + \sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p \text{ prime}} \left(1 - \sum_{\alpha\geq 1} \frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right)$$

and deduce that

$$C_{\Gamma,t} = \delta_\Gamma \left(1 + \sum_{\substack{\eta|\sigma_\Gamma\\ \eta\neq 1}} \frac{\sum_{\alpha\geq\gamma_\eta} \frac{2^t-1}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|}}{\sum_{\alpha\geq 1} \frac{2^t-1}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|}} \prod_{p|2\eta} \left(1 + \left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)^{-1}\right)^{-1}\right)$$

where $\gamma_\eta = \max\{1+t_\eta, v_2(\delta(\eta))\}$ and this completes the proof. □

5 Proof of Corollary 3

Let Γ be a finitely generated subgroup of $\mathbb{Q}^+$ of rank r and let $(a_1, ..., a_r)$ be a $\mathbb{Z}-$basis of Γ. We write $\mathrm{Supp}(\Gamma) = \{p_1, ..., p_s\}$. Then we can construct the $s \times r-$matrix with coefficients in $\mathbb{Z}$:

$$M(a_1, ..., a_r) = A = \begin{pmatrix} \alpha_{1,1} & \dots & \alpha_{1,r} \\ \vdots & & \vdots \\ \alpha_{s,1} & \dots & \alpha_{s,r} \end{pmatrix} \tag{30}$$

defined by the property that $|a_i| = (p_1)^{\alpha_{1,i}}...(p_s)^{\alpha_{s,i}}$. It is clear that $s \geq r$ and that the rank of the matrix $M(a_1, ..., a_r)$ equals r. For all $i = 1, ..., r$ we define the $i-$th exponent of Γ by

$$\Delta_i = \Delta_i(\Gamma) = \gcd(\det A : A \text{ is a } i \times i \text{ minor of } M(a_1, ..., a_r))$$

and we also set $\Delta_0 = 1$. For $m \in \mathbb{N}$, we have (see [1, Proposition 2])

$$|\Gamma(m)| = \frac{m^r}{\gcd(m^r, m^{r-1}\Delta_1, ..., m\Delta_{r-1}, \Delta_r)}$$

and in particular, for every prime power p^α, we have

$$|\Gamma(p^\alpha)| = p^{\max\{0, \alpha - v_p(\Delta_1), ..., (r-1)\alpha - v_p(\Delta_{r-1}), r\alpha - v_p(\Delta_r)\}}.$$

Proof of Corollary 3. Let Γ be generated by prime numbers $p_1, ..., p_r$, since Δ_i's are 1 we have $|\Gamma(k)| = k^r$ and $t_\eta = 0$ for all $\eta \mid \sigma_\Gamma = p_1 \cdots p_r$ and

$$\gamma_\eta = \begin{cases} 1 & \text{if } \eta \equiv 1 \bmod 4 \\ 2 & \text{if } \eta \equiv 3 \bmod 4 \\ 3 & \text{if } \eta \equiv 2 \bmod 4. \end{cases}$$

Furthermore

$$\sum_{\alpha\geq\gamma_\eta}\frac{1}{2^{2\alpha-1}|\Gamma(2^\alpha)|}=\frac{1}{2^{(\gamma_\eta-1)(r+2)}}\sum_{\alpha\geq 1}\frac{1}{2^{2\alpha-1}|\Gamma(2^\alpha)|}$$

and since $|\Gamma(k)|=k^r$ for all $k\in\mathbb{N}^+$, we have that

$$\sum_{\alpha\geq 1}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}=\frac{p}{p^{r+2}-1}.$$

Hence, if we let

$$C_r=\prod_p\left(1-\frac{p}{p^{r+2}-1}\right),$$

then

$$C_{\langle p_1,\dots,p_r\rangle}=C_r\left(1+\sum_{\substack{\eta|p_1\cdots p_r\\ \eta\neq 1}}\frac{1}{2^{(\gamma_\eta-1)(r+2)}}\prod_{\ell|2\eta}\frac{\ell}{\ell+1-\ell^{r+2}}\right)$$

and this completes the proof. □

6 Proof of Corollary 4

Proof of Corollary 4. If we set $k_p=\max\{v_p(\Delta_r/\Delta_{r-1}),\cdots,v_p(\Delta_1/\Delta_0)\}$ then for $\alpha\geq k_p$, $|\Gamma(p^\alpha)|=p^{r\alpha-v_p(\Delta_r)}$. Hence

$$\sum_{\alpha\geq 1}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}=\sum_{\alpha=1}^{k_p}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}+\frac{p^{v_p(\Delta_r)+1-(r+2)k_p}}{p^{r+2}-1}\in\mathbb{Q}.$$

In particular, if $p\nmid\Delta_r$, then $k_p=0$ and $|\Gamma(p^\alpha)|=p^{\alpha r}$ for all $\alpha\geq 0$ and

$$\sum_{\alpha\geq 1}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}=\frac{p}{p^{r+2}-1}.$$

Therefore

$$C_\Gamma=r_\Gamma\prod_{p\nmid\Delta_r}\left(1-\frac{p}{p^{r+2}-1}\right)$$

where

$$\begin{aligned} r_\Gamma\quad &=\prod_{p|\Delta_r}\left(1-\sum_{\alpha\geq 1}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right)\\ &\times\left(1+\sum_{\substack{\eta|\sigma_\Gamma\\ \eta\neq 1}}S_\eta\prod_{p|2\eta}\left(1-\left(\sum_{\alpha\geq 1}\frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right)^{-1}\right)^{-1}\right)\in\mathbb{Q}. \end{aligned}\tag{31}$$

Finally C_Γ is a rational multiple of

$$C_r=\prod_p\left(1-\frac{p}{p^{r+2}-1}\right)$$

and this concludes the proof. □

7 Proof of Theorem 1

The proof use the methods of Kurlberg and Pomerance [3, Theorem 2].

Proof of Theorem 1. Let $z = \log x$. We have

$$\sum_{p\le x} |\Gamma_p|^t = \sum_{\substack{p\le x\\ \operatorname{ind}(\Gamma_p)\le z}} |\Gamma_p|^t + \sum_{\substack{p\le x\\ \operatorname{ind}(\Gamma_p)> z}} |\Gamma_p|^t = A + E,$$

say. We write $|\Gamma_p|^t = \frac{(p-1)^t}{\operatorname{ind}^t(\Gamma_p)}$ and use the identity $\frac{1}{\operatorname{ind}^t(\Gamma_p)} = \sum_{uv|\operatorname{ind}(\Gamma_p)} \frac{\mu(v)}{u^t}$, after splitting the sum we have

$$\begin{aligned} A &= \sum_{p\le x}(p-1)^t \sum_{\substack{uv|\operatorname{ind}(\Gamma_p)\\ uv\le z}} \frac{\mu(v)}{u^t} - \sum_{\substack{p\le x\\ \operatorname{ind}(\Gamma_p)>z}} (p-1)^t \sum_{\substack{uv|\operatorname{ind}(\Gamma_p)\\ uv\le z}} \frac{\mu(v)}{u^t} \\ &= A_1 - E_1, \end{aligned}$$

say. The main term is A_1, after switching the summation and applying partial summation and using Lemma 6 on GRH, we have

$$A_1 = \operatorname{li}(x^{t+1}) \sum_{uv\le z} \frac{\mu(v)}{u^t[\mathbb{Q}(\zeta_{uv}, \Gamma^{1/uv}) : \mathbb{Q}]} + O\left(x^{t+\frac{1}{2}} \log x \sum_{n\le z} \left| \sum_{uv=n} \frac{\mu(v)}{u^t} \right| \right).$$

The inner sum in the O-term is bounded by $\frac{\varphi(n)}{n}$ so that the O-term above is $O\Big(x^{t+\frac{1}{2}} \log^2(x)\Big)$. Next we use the elementary fact $J_t(\operatorname{rad}(k)) = J_t(k)\left(\frac{\operatorname{rad}(k)}{k}\right)^t$ and $\sum_{v|k} \mu(v)v^t = \prod_{p|k}(1-p^t) = (-1)^{\omega(k)} J_t(\operatorname{rad}(k)) = (-1)^{\omega(k)} \frac{J_t(k)(\operatorname{rad}(k))^t}{k^t}$. So

$$\sum_{uv=k} \frac{\mu(v)}{u^t[\mathbb{Q}(\zeta_{uv}, \Gamma^{1/uv}) : \mathbb{Q}]} = \sum_{v|k} \frac{\mu(v)v^t}{k^t[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]} = \frac{(-1)^{\omega(k)} J_t(k)(\operatorname{rad}(k))^t}{k^{2t}[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}])}.$$

Let $C_{\Gamma,t} := \sum_{k\ge 1} \frac{J_t(k)(\operatorname{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]}$, after applying Corollary 7, finally we have

$$A_1 = \operatorname{li}(x^{t+1})\left(C_{\Gamma,t} + O\left(\frac{1}{z^r}\right)\right).$$

It remains to estimate the error terms E and E_1. Applying Theorem 9:

$$E \ll \frac{x^t}{z^t}\frac{\pi(x)}{z^r}.$$

In order to estimate E_1, we calculate

$$\left| \sum_{\substack{uv|n\\ uv\le z}} \frac{\mu(v)}{u^t} \right| \le \sum_{u|n} \frac{1}{u^t} \sum_{\substack{v|n\\ v\le z}} 1 \le \frac{\tau(n)\sigma_t(n)}{n^t},$$

so

$$E_1 \le \sum_{z<n} \frac{\tau(n)\sigma_t(n)}{n^t} \sum_{\substack{p\le x\\ n|\operatorname{ind}(\Gamma_p)}} (p-1)^t.$$

Then applying Lemma 6 and Corollary 7 we obtain that

$$E_1 \ll x^t \pi(x) \sum_{z<n} \frac{\tau(n)\sigma_t(n)}{n^t \varphi(n) n^r}.$$

Let $g(n) := \frac{\tau(n)\sigma_t(n)}{n^{t-1}\varphi(n)}$, $\sum_{p \le x} g(p) = (2+o(1))\frac{x}{\log x}$. Using Lemma 10 (for in our case τ is 2), we have

$$\sum_{n\le x} g(n) = \left(\frac{1}{e^{\gamma 2}} + o(1)\right) \frac{x}{\log x} \prod_{p \le x} \left(1 + \frac{p}{(p-1)(p^t-1)} \sum_{\nu \ge 1} \frac{(\nu+1)(p^{\nu t + t} - 1)}{p^{\nu t + \nu}}\right).$$

To make the product convergent we add a correction factor, and invoke Merten's third formula, we have

$$\sum_{n \le x} g(n) \sim x \log x.$$

Let $G(n) := \sum_{n \le x} g(n)$ using partial summation, we have

$$\sum_{z<n} \frac{g(n)}{n^{r+1}} = \lim_{T\to\infty} \left(\frac{G(T)}{T^{r+1}} - \frac{G(z)}{z^{r+1}}\right) - \int_z^\infty G(u) \frac{d}{du}\left(\frac{1}{u^{r+1}}\right) \ll \frac{\log z}{z^r}.$$

Therefore, we obtain

$$E_1 \ll x^t \pi(x) \frac{\log z}{z^r}.$$

We have chosen $z = \log x$, finally we have

$$\sum_{p \le x} |\Gamma_p|^t = \mathrm{li}(x^{t+1}) C_{\Gamma,t} + O\left(\frac{x^{t+1} \log\log x}{(\log x)^{r+1}}\right).$$

$\square$

8 Numerical Examples

In this section we compare some numerical data. The tables compares the value of C_Γ as predicted by Corollary 3 with

$$A_\Gamma = \frac{\sum_{p \le 10^{10}} |\Gamma_p|}{\sum_{p \le 10^{10}} p}.$$

We consider the following cases:

- $\Gamma_r = \langle 2, ..., p_r \rangle$, the group generated by the first r primes
- $\Gamma'_r = \langle 3, ..., p_{r+1} \rangle$, the group generated by the first r odd primes.
- $\Gamma''_r = \langle 5, ..., p''_r \rangle$, the group generated by the first r primes congruent to 1 modulo 4.

r	1	2	3	4	5	6	7
A_{Γ_r}	0.5723625220	0.8234145762	0.9219692467	0.9638944667	0.9828346715	0.9916961670	0.9959388895
C_{Γ_r}	0.5723602190	0.8234094709	0.9219688310	0.9638925514	0.9828293379	0.9916891587	0.9959315465
$A_{\Gamma'_r}$	0.5797271743	0.8249081874	0.9220326599	0.9639044730	0.9828352799	0.9916947130	0.9959372205
$C_{\Gamma'_r}$	0.5797162295	0.8249060912	0.9220306381	0.9639002343	0.9828302996	0.9916892783	0.9959315614
$A_{\Gamma''_r}$	0.5856374600	0.8246697078	0.9220170449	0.9639045923	0.9828329969	0.9916930151	0.9959357111
$C_{\Gamma''_r}$	0.5856399683	0.8246572843	0.9220082264	0.9638982767	0.9828301305	0.9916892643	0.9959315465

Acknowledgement: This paper is part of the Doctorate thesis at the Università Roma Tre.

References

[1] Cangelmi, L. and Pappalardi, F., *On the r–rank Artin Conjecture II*, J. Number Theory **75** (1999), 120–132.

[2] Hooley, C., *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[3] Kurlberg, P. and Pomerance, C., *On a problem of Arnold: the average multiplicative order of a given integer*, Algebra and Number Theory, **7** (2013), 981-999.

[4] Matthews, C. R., *Counting points modulo p for some finitely generated subgroups of algebraic groups*, Bull. London Math. Soc. **14** (1982), 149–154.

[5] Moree, P., *Artins primitive root conjecture -a survey-*, Integers **12A** (2012), A13, 100pp.

[6] Pappalardi, F., *Divisibility of reduction in groups of rational numbers* , Math. Comp. to appear

[7] Serre, J. P., *Quelques applications du theor'eme de densite de Chebotarev*, Inst. Hautes Etudes Sci. Publ. Math. **54** (1981), 323-401.

[8] Wirsing, E., *Das asymptotische Verhalten von Summen uber multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.